Legal admissibility of electronic evidence

Leroux, Olivier

Published in:
International review of law computer and technology

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

INTERNATIONAL REVIEW OF LAW COMPUTERS
& TECHNOLOGY, VOLUME 18, NO. 2, PAGES 193–220, JULY 2004

Carfax Publishing
Taylor & Francis Group

Legal Admissibility of Electronic Evidence[1]

OLIVIER LEROUX

ABSTRACT *The use of computers and digital media in unlawful activities has increased so dramatically that investigation of any criminal activity may nowadays produce electronic evidence. However, the rapid growth in the number of criminal cases involving electronic evidence has all-too-often found law enforcement and the judiciary badly prepared to deal with the new issues created by this evidence. The gathering, conservation, communication and presentation of the computer-derived evidence must fulfil legal requirements with regard to the admissibility of the evidence. Electronic evidence that was gathered in a way that was not in accordance with the law will be declared inadmissible and be ruled out of court. This report aims to briefly present the core principles of the law when handling electronic evidence. Therefore, this paper examines the conditions of admissibility of evidence in four European countries. In order to be complete and to give an interesting pan-European view on the question, the English law system has been chosen to illustrate the functioning of the rules relating to the evidence in a country ruled by common law.*

1. General Introduction and Objectives

The CTOSE (Cyber Tools for On-line Search for Evidence) project aims to make it possible, while respecting security and privacy requirements, to produce evidence of disputed electronic transactions that is comprehensible to those called upon to make judgements about the transactions concerned, and is sufficiently reliable and well authenticated to be accepted as proof of an electronic event that has happened.

In order to avoid polluting the evidence, the gathering, conservation, communication and presentation of the evidence must fulfil legal requirements with regard to the admissibility of the evidence.

Compromised evidence could have major consequences on the judicial trial if its admissibility is disputed or, to a lesser extent, if it is not considered as relevant. In English

Correspondence: Olivier Leroux, Centre de Recherches Informatique et Droit (CRID), University of Namur, Rue de Bruxelles, 61 B5000 Namur, Belgium. Email: oleroux@fundp.ac.be.

ISSN 1360-0869 print/ISSN 1364-6885 online/04/020193-28 © 2004 Taylor & Francis Ltd
DOI: 10.1080/1360086042000223508

law, the violation of evidence rules do not prevent the accusation from producing the litigious proof; but the court retains the discretionary ability to accept it or to refuse it. In French inspired systems (e.g. Belgian and Italian systems), on the other hand, inadmissible evidence must be declared null and void: The nullity of subsequent procedure could be implied from inadmissible evidence.

Inadmissible evidence could be not only considered as of no use for the trial, but it could also, in some cases, pollute the subsequent proceedings based on it, rendering these proceedings null and void. Issues relating to the admissibility of the evidence are therefore to be distinguished from questions relating to the relevance of the proofs, the most relevant evidence potentially being more prejudicial for the whole judicial process (whether it be civil or criminal) than no evidence at all.

It is therefore necessary to examine the main principles of evidence rules in several Member States of the European Union (EU) in order to ensure that the CTOSE process model conforms with legal rules of the evidence. A primary distinction must be made between continental law countries (Belgium, France and Italy) and common law countries (England).

Issues concerning the admissibility, similarities and differences in the rules of evidence in criminal law must be examined. There are first similarities between the systems because presumption of innocence exists in all, even if it is often limited in special situations. Differences however, exist about freedom or restriction of the types of proof. In France, Italy and Belgium, the principle of freedom prevails, whereas the Common Law systems refuse hearsay evidence (with many exceptions, however). In this case the rules concerning the manner and procedure for submitting evidence are applied differently, for instance those concerning discovery or the sanction for illegally obtained evidence. Finally, regarding the weight of evidence, in some systems the court is completely free to interpret evidence ('in-time conviction'), while in others, it is bound by such rules as those requiring corroborative evidence.

For what concerns the admissibility of the electronic evidence in civil matters, continental law systems depend on a strict regulation of the evidence, where common law countries (infrequently divided into private and public law) consider in principle every piece of evidence admissible as far as it is relevant, subject to exceptions among which are hearsay evidence and the best evidence rule.

Consequences of inadmissible evidence in civil cases may probably be seen as less 'dangerous' than the ones in criminal procedure. It is nevertheless true that invalid (inadmissible) evidence risks making it impossible for the plaintiff to prove his assertions, making any judicial action pointless.

The CTOSE project focuses on the process of handling electronic evidence in the case of disputed electronic transactions. This covers cyber crimes as well as e-business litigations.

The purpose of CTOSE is then to make possible (legally speaking) the production of electronic evidence in the case of disputed electronic transactions (communications) while respecting security and privacy requirements. This evidence must be comprehensible to those called upon to make judgements about the transactions concerned, and must be sufficiently reliable and well authenticated to be accepted as proof of an electronic event that has happened.

The objectives of legal 'deliverables' are to ensure the compliance of the full processing of evidence (gathering, conservation and production) with EU legislation and to demonstrate how far illegal processing of evidence may undermine its validity. It is also to validate and to assess the technical means of processing evidence with regard to data protection and confidentiality as stated by EU legislation.

This 'deliverable' aims to analyse the legal requirements with regard to the admissibility of electronic evidence as well as the influence of law infringement when processing evidence.

This report examines the conditions of admissibility of evidence in four European countries. In order to be complete and to give an interesting pan-European view on the question, the English law system has been chosen to illustrate the functioning of the rules relating to the evidence in a country ruled by common law.

2. Legal Requirements with Regard to the Admissibility of Electronic Evidence

2.1. Introduction

In every judicial trial, gathered evidence will form the cornerstones upon which serious decisions will be made. Computers provide large resources for the discovery of evidence—resources that have been largely untapped by litigants.[2] Computers, and the various media in which computer-generated information is stored, provide a unique window into company's or individual's correspondences, data, statistics ... and generate, sort and store huge amounts of information, while providing a source of information that may not exist in paper form.[3]

In criminal cases, successful investigations in the field of information technology require a variety of information. Without evidence, or in the case of invalid evidence, and in the absence of a confession, prosecutions will not often succeed.[4] In civil cases, all parties will attend to base their contensions on reliable and valuable pieces of evidence to be successful. To avoid being ruled out of court, the parties must put forward elements that fulfil legal requirements with regard to the admissibility of the evidence.

It is therefore essential to ensure in both types of cases that computer-related evidence was collected, preserved and transmitted in accordance with legal requirements regarding the admissibility of the evidence.

However, because of the intangible character of the electronic evidence, many cases do not even make it to court because of compromised evidence. The replacement of visible and corporeal objects of proof by invisible and intangible evidence in the field of information technology, does indeed not only create practical problems, but also opens up new legal issues.

Among the practical issues created by the digital evidence, it is mainly emphasized that the main object of interest is usually computerized data stored on corporeal data carriers.[5]

First, it is very volatile: data (document, record, logs, etc.) can be changed easily simply by typing a few keystrokes and often this can be done without leaving manifest traces. Then, it can be easily unintentionally altered without obvious traces. Very often, an investigation may need to attempt to recover data that have been deleted—is the court simply to accept this as 'magic'?[6] Second, the digital evidence is most fragile: it can be very sensitive and easily destroyed by inexperienced access and handling (diskettes and hard drives can be destroyed or rendered useless by electromagnetic forces, improper handling and storage). This is the reason why the computer and its media must be handled in a way that ensures that no possible evidence is damaged, destroyed or altered. Computer data, which is the main object of computer crime, is characterized by an extreme mobility which exceeds by far the mobility of persons, goods or other services: international computer

networks can transfer huge amounts of data around the world in a matter of seconds. The work produced on a computer based in one country can resurface in some other territory.[7] Finally, the gathering of evidence will suppose a strong computing knowledge as well as legal capacities to collect this evidence in respect to legal requirements: its admissibility before a court must not be altered. The forensic investigator has to be highly trained if the information gathered is to be available in a usable form, but he also has to be aware of legal requirements relating to the evidence. Polluted evidence could indeed be ruled out of court and prevent subsequent proceedings. This is highly novel, and creates problems of explanation as well as of forensic testing.[8]

However, these particularities do not exempt the electronic evidence from legal requirements relating to the evidence in the real world. Computer-derived evidence has to have all attributes of conventional evidence: it must be admissible (conform to legal rules to be put before a court), authentic (possible to positively tie evidentiary material to the incident), complete (as much as possible), reliable (there must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity), and believable (understandable by a court).[9]

Among the legal difficulties generated by digital evidence for those who wish to rely on it,[10] it is strongly advisable above all to be first aware of the consequences resulting from an improper gathering, collection or transmission of the evidence.

An empirical differentiation between the various types of information is essential, since most of the criminal procedure laws in many countries are based on express provisions of specific coercive powers. Most legal systems differentiate the following issues: the possibilities of monitoring publicly available facts, the powers of entry and search of premises, the powers of seizure and retention, the duty of witnesses to testify, the duty of witnesses to surrender existing means of evidence and the powers of wiretapping.[11] Since most of the traditional provisions were elaborated with respect to the physical world and not especially designed for intangibles and for the special needs of the information society, it is questionable, in many legal systems, whether or not the traditional coercive powers are adequate for all aspects of investigations in computerized environments.

The main aim of this report is to analyse the legal issues relating to the admissibility of the electronic evidence by the analysis of legal rules in the EU and more specifically in Belgium, France, UK and Italy. In other words, the objectives of this study are to bring to light the conditions to be followed to make pieces of electronic evidence valid before a court in regard to the rules applicable in several jurisdictions. Therefore, we will consider the different European legal systems in the way they treat the admissibility of the electronic evidence.

For each national law system examined, the legal requirements with regard to the e-evidence will be determined for any disputed electronic transaction. This means that the legal requirements will cover private law cases as well as criminal cases.[12]

In order to be as coherent as possible for non-lawyers, this report uses common terms as much as possible or, when it refers to legal terms, holds explicit definitions of the concepts used.[13]

2.2. Core Principles of the Law of Evidence

2.2.1. *Evidence—law of evidence: definitions.* Since there is no legal definition of the evidence, evidence can be defined as: 'information by which facts tend to be proved'.

Evidence is thus the means by which factual ingredients of an offence (because of which proceedings are started) or a civil litigation can be proved, in order to succeed.

In this context, evidence law strives to ensure that only reliable evidence is permitted for provision to judicial courts and other decision makers in legal, administrative and related proceedings.[14] The law of evidence is the body of legal rules regulating the means by which facts may be proved in courts of law and arbitrations in which the strict rules of evidence apply.[15] The law of evidence intends to regulate these means and answer questions arising from its application: who has to produce evidence?, (who has the burden of the proof?), are all means of proof admissible?, (what are the consequences of a non-admissible evidence?), how far is a proof relevant? The law of evidence is a complicated issue and varies from one country to another. For this reason, the content of this present report has to be seen as an overview of the main concepts, which could lead to further developments.

2.2.2. *Structure.* The legal requirements with regard to the admissibility of evidence from computer records in courts depend to a great extent on the underlying fundamental principles of evidence in respective countries.

Two main groups of countries are traditionally differentiated: the continental law countries on the one hand (France, Germany, Italy, Spain, Belgium, etc.) which developed a proceedings presided over by an interrogating judge; and the common law countries on the other hand (USA, UK), which developed an accusatory procedure (adversary system of trial). This distinction generates deep theoretical differences with regard to the rules regulating evidence.

Moreover, when analysing questions concerning the evidence in several legal systems, it is a widespread practice in continental law countries to distinguish private law rules (dominated by the system of the legal proof) from criminal law rules (where the free introduction and evaluation of the evidence in continental law countries prevails).[16] Civil law nations indeed often employ entirely separate hierarchies of courts for public and private law. Evidence issues are therefore very different in private law and in criminal law cases.

This is the reason why legal requirements regarding electronic evidence will be analysed in both continental law and common law countries. This analysis will be made after a short presentation of the key concepts of the law of the evidence (admissibility, relevance, burden of the proof). Each chapter has been divided in two sections, respectively dedicated to electronic evidence in private law and criminal law.

2.2.3. *Key concepts: burden of proof, admissibility, relevance.* Burden of proof, admissibility and relevance are three different notions of law of evidence, which must be clearly differentiated in order to avoid confusion.

2.2.3.1. *Burden of proof.* The expression 'burden of proof' is self-explanatory: it is the obligation to prove. It aims to determine which party has to prove which fact.

In English law, there are two principal kinds of burden: the legal burden and the evidential burden. The legal burden may be defined as the obligation imposed on a party by a rule of law to prove a particular fact at issue. The rules of substantive law determine which party bears the legal burden of the proof in relation to any given fact at issue. The evidential burden may be defined as the obligation on a party to adduce sufficient evidence of fact to justify a finding on that fact in favour of the party so obliged.

In criminal cases, generally speaking, the legal burden of proving any fact essential to the prosecution case rests upon the prosecution and remains with the prosecution throughout the trial. Therefore, the accused bears no legal burden in respect of the essential ingredients of an offence, whether they are positive or negative and whether or not he denies any or all of them. The adages of the civil law, '*actori incumbit probatio*' and '*onus probandi incumbit ei qui dicit*' are, in a way, also applicable in criminal cases. It means that the prosecutor (*Procureur*—or *Ministère public*) must prove the infraction he is prosecuting. Furthermore, because of the legal innocence presumption (dominating all questions relating to the burden of the proof in criminal cases[17]), the prosecuted person does not have to prove his innocence: '*in dubio pro reo*'. It is the prosecutor who is in charge of proving the guilt of the defendant.[18] If the guilt is not sufficiently and indisputably established, the defendant must be acquitted.[19]

In civil cases, the general rule is that he who asserts something must prove it. The legal burden of proof will generally lie on the party asserting the affirmative of such an issue.

2.2.3.2. *Admissibility*. The admissibility of evidence is a matter of law for the judge. He has to take into account probative elements lawfully acknowledged as admissible with regard to the purpose of the dispute.[20] This concerns the validity of the evidences brought before a court. This does not mean that an admissible evidence will in any case influence the decision of the judge. An admissible evidence may indeed be irrelevant, but this means that the judge will be forced to examine this element.

In principle, in English law, all evidence that is sufficiently relevant to prove or disprove a fact at issue and which is not excluded by the law of evidence is admissible.[21] We will see that the rules relating to the admissibility of the evidence vary from one legal subject to another.

2.2.3.3. *Relevance*. Relevance is a matter of appreciation by the judge.[22] The relevance is usually defined as: 'any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present or future existence or non-existence of the other'.[23] Evidence is therefore relevant if it is logically probative or disprobative of some matter that requires proof, or makes the matter that requires proof more or less probable. Relevance is a question of degree determined by common sense and experience.

2.2.4. The electronic evidence in civil cases. The possibilities of obtaining evidence by civil proceedings, especially by preliminary injunctions and civil seizure, vary considerably from one country to another.

2.2.4.1. *Continental law countries (Belgium, France, Italy). Burden of proof*—In principle, the burden of proof rests with the plaintiff (complainant) in civil cases: '*Actori incumbit probatio; reus in excipiendo contractus fit actor*'[24] (he who asserts must prove). So, for example, the legal burden of proving a contract, its breach and consequential loss lies on the claimant, and the legal burden of proving a defence that goes beyond a simple denial of the claimant's assertions, such as discharge by agreement or by frustration, lies on the defendant.

Articles 1315 of the Belgian and French civil codes lay down that the one who claims the execution of an obligation has to prove the existence of this obligation, and, reciprocally, the one who asserts that he is free of his obligation has to prove the payment or the fact that fulfilled his obligation (the one who claims he fulfilled his obligation must likewise bring the evidence of that execution).[25] Article 870 of the Belgian procedural code states that each party has the burden of proving the elements it is asserting. These dispositions regulate the burden of proof as well as the risk of the impossibility to prove: it settles which party is going to fail if a doubt remains.[26]

However, it happens in some cases that the legislator decides, by way of a legal presumption, to rely on someone else for the obligation of bringing the evidence.

Moreover, the principle of the burden of proof according which the claiming person has to prove may be shortcut by a convention. Two or more persons are allowed to decide, under the conditions they agreed, that the burden of proof would lay on a person they indicated. Such a convention may only occur when the rules of evidence are not imposed in an imperative way by the law. We will see that the French law adapting the rules of evidence to information technologies and to the electronic signature introduced this conventional exception into the civil code.[27]

Admissibility—When considering rules relating to the admissibility of the evidence in private law cases, it is advisable to distinguish civil cases from commercial cases.[28] Commercial cases fall under the rules of evidence in commercial law (*the Law Merchant*), according which contracts or obligations may be proved by any means of evidence. Civil cases, however, involving non-merchants, fall under the strict rules of the civil evidence, which are held in the civil code. In case of mixed contracts (involving merchants as well as non-merchants), the contract gets ruled as follows: the *non-merchants* (individual, organization or company) are allowed to use against *merchants* every means of proof to establish the legitimacy of their assertion or counter the presumption offered by the civil code (see *infra*), while *merchants* may only use against *non-merchants* written documents, as described in the civil code.

In commercial law, the evidence is usually seen as free: any means of proof is in principle admissible. The French commercial law establishes the 'freedom of evidence' as a core principle, to prove legal facts and legal acts as well (article 109 of the *Code de commerce*). Nevertheless, it is the judge who decides if the evidence brought to him by the plaintiffs is relevant to prove their assertions. The Belgian commercial code lays down (article 25) that the meaning of proof is free in commercial matters except for some situations where a written proof is required (for example to establish the reality of an insurance contract, a bill of exchange, etc).

Contrary to commercial law, civil law is mostly run by the system of legal evidence. It means that the law determines which sort of evidence is admissible. Once admissible, the judge has to consider the evidence as proving the assertion of the person who brought it (relevance). However, whereas previously the judge has had quite a passive role, he now has the possibility to order any instruction measures when he cannot rule on the case for lack of elements. Nevertheless, the law must have allowed these measures. The judge may order these on his own, or when asked by one of the plaintiffs or one of the suited persons, although he is not obliged to accede to such a request (see articles 10 and 143 of the French *Nouveau Code de procédure civile*).[29]

For a very long time, the written document used to be the means of proof dominating the systems of civil law in the continental law countries. According to this important legal tradition, articles 1341 of the Belgian and French civil codes demand a previously prepared written evidence for any act (each convention, obligation, in general, or even voluntary deposit) exceeding an amount of money fixed by decree (5000 former French francs—

€800—in the French civil code; 15,000 former Belgian francs—€375 in the Belgian civil code).[30] The necessity of a written document laid down by article 1341 of the civil code (in France and in Belgium) has some limitations. It has already been said that it does not concern the commercial law. It is also obvious that such an obligation only regards the legal acts and not the legal facts, which cannot be foreseen. Moreover, this principle finds some exceptions when there is a moral impossibility to obtain a written act (e.g. in the case of an affective or friendship relation), when the original document has been lost but a valid copy is available or when there is a '*commencement de preuve par écrit*'. This last concept concerns any written document that emanates from the person against whom the legal request is intended. In all these cases, other means of proof can be used, notably testimony and presumptions.[31]

The written documents demanded by the civil code as evidence can be of two types, distinguished by the solemnity of their making and by the different effects they cause: the notarial deed (*acte authentique*), which must have been received by a public officer allowed to act in the place where the act was drawn up (article 1317 of the *Code civil*), and in the respect of all the required solemnity; and the private agreement (*acte sous seing privé*), which is a written document drawn up under the liability of the persons who signed it, without any intervention of a public officer. This document is not legally certified.

Because of the particularities of the digital environment, and in order to conform electronic data to legal requirements in civil cases, civil codes have suffered a few adaptations. The domination of the written document as a means of proof had indeed lead to a main problem in that electronic context: how far can a written text, which does not appear on paper, be considered as a written document in the sense of the civil code? The monopoly of paper made the jurists think that evidence could not be written in any other medium. Now that such a monopoly has disappeared, this question must be rethought.

On 13 December 1999, the European Parliament and the Council adopted the European directive on a Community framework for electronic signatures[32] obliging all Member States to adapt their internal legislation to its dispositions. According to this directive, legal systems of Member States must recognize digital signatures (fulfilling specific requirements) as admissible and as valuable as a handwritten signature.

In order to cope with this difficulty and to model its legislation to international obligations,[33] the French Parliament adopted on 13 March 2000 a specific law in order to adapt the law of evidence to information technologies.[34] The Belgian Parliament did likewise, by adopting two different laws, respectively dedicated to the electronic signature and trusted third parties (*autorités de certification*).[35] The Italian Parliament took similar action.[36]

The purpose of these laws was to confer to the electronic document and the electronic signature the same legal value that written-paper documents have.

The transformations brought to the civil codes in order to make the electronic evidence admissible concern the notion of written documents and its relevance.

(a) *Widening of the notion of written document.* The definition of the written document has been transformed following the principles of the technical neutrality and the non-discrimination regarding any supports or media. Therefore, the notion of written document is now extensive and includes also, but not only, electronic documents.

The new article 1316 of the French civil code lays down that written evidence consists of a series of letters, characters, numerals or any other signs or symbols that have an intelligible signification, whatever their support or their means of transmission. By intelligible signification, the legislator means that the document can be presented in a readable and understandable way.[37]

(b) *Relevance of electronic documents.* Since the French law of 13 March 2000 was adopted, the support of the document does not matter anymore: the electronic document has now the same relevance as a paper document (new article 1316-3 of the French civil code). According to the principles of technical neutrality and non-discrimination regarding supports or media, there is no hierarchy between the different sorts of documents.

However, to be considered as a written document, the electronic one must respect two conditions (new article 1316-2 of the French civil code). First, the electronic document must identify the person from whom it emanates. Second, the integrity of the electronic document must be guaranteed, which means it has to be established and conserved in conditions that preserve it from any modifications.[38]

The institution of the electronic signature. After having established the admissibility of the electronic document as a means of proof, the French law of 13 March 2000 included the electronic signature in the legal notion of signature in general. Aimed as a transposition of the EU Directive on electronic signatures,[39] the law follows the same approach: definition of the function of the signature and reliability of the signature depending on the safety brought by the certification providers.

So, new article 1316-2, *al.* 1, of the civil code lays down that an electronic signature must allow the identification of the signing party. It must also be the manifestation of the agreement between the parties to the convention. This article specifies as well that the electronic signature must consist of a reliable link between the act and the person who signed it. When conditions have been fixed by decree about the creation of the signature, the identification of the person who signed and the integrity of the act have been fulfilled, the reliability of the signature is presumed. To respect those last conditions, the signature must be guaranteed by a signature certificate provider (trusted third party). Those certificate providers have themselves to observe any minimal safety conditions in order to be allowed to operate.[40]

So far the electronic signature respects those conditions, it has the same relevance as a paper-one, according to the principle of technological neutrality and non-discrimination regarding to the type of supports or media. In this way, even the electronic signature inserted by a public officer has the same effect it would have on paper support: the authenticity of the act. Any kind of digital signature has thus to be considered as admissible by the judge.

Relevance—The relevance of the notarial deed (*acte authentique*) is huge, if all the conditions have been fulfilled and all the details that the public officer drew up (i.e. date, presence of the different persons, payment, etc.) are considered truly. The only way to counter it is to institute difficult proceedings against the notarial deed called the '*inscription de faux*'.[41]

The private agreement's (*acte sous seing privé*) relevance is not as important as that of the notarial deed. The private agreement's details are trusted evidence but only between the persons who signed the document. As regards to third parties, probative value of the document depends on the certainty of the date, which is gained by the death of the person who signed it, by a public officers' record of its existence or by the registration of the document.[42]

Concerning electronic documents that include an electronic signature, new article 1316-2 of the French civil code tackles the question of a conflict between two documents (one handwritten and the other one electronic). After having established the validity of particular conventions concerning the means of proof, this article gives the judge the ability to appreciate which document has to be considered as relevant. The judge must thus determine the most convincing document (*'le titre le plus vraisemblable'*) whether and what its support consists of.[43]

2.2.4.2. *Common law country (UK—England).* The English court system has been refined in the past century. The courts nevertheless retain characteristics associated with their structure as formed in the three first centuries of the previous millennium. It remains essentially a unitary system where all courts, both civil and criminal, lead to the Court of Appeal and the House of Lords. Ordinary courts in England most generally are classified as superior or inferior. Inferior court jurisdiction is limited both geographically and according to the nature of subject matter and includes those civil and criminal courts that decide the vast majority of disputes, the county and magistrates' courts, respectively. Superior court jurisdiction is country wide, and consists of the Crown court, High Court, Court of Appeal and House of Lords.

English law of evidence remains notorious for its complexity and excessive technicality.

Burden of proof—Once governed by an almost mystical unwritten scheme, for a little more than a century, English civil procedure has now been substantially codified.[44] Rules of the Supreme Court now regulate most civil proceedings in the Supreme Court, and there are corresponding rules for the county courts and for criminal proceedings in the magistrates' courts.

The English trial is an oral process (although the oral process also is mandated by the nature of the trial today, the use of written witnesses and expert statements has reduced the oral adversary system). Counsel for the plaintiff makes a statement of his client's case and next calls his witnesses, each of whom may be cross-examined by defence counsel and re-examined by the plaintiff's counsel. When the plaintiff's case has been presented, the defence initiates a similar presentation of witnesses, with cross-examination by the plaintiff. However, the English civil trial judge sometimes plays an active role in directly questioning the parties. Judicial participation is important in a civil trial where either party may decide not to introduce evidence. The judge may be able to extract what one counsel prefers not to mention, and the others ignore.

Admissibility—Principle. English law of evidence shares with many others common law jurisdictions a commitment to exclusionary rules that generally have no counterparts in civilian systems, where the dominant principle is that of the free appreciation of the evidence. English lawyers have thus to be concerned, not just with the quality of the evidence in terms of its relevance and capacity to convince a court or a tribunal of the facts with which it deals, but also with its classification and formal admissibility. Evidence may sometimes be ruled inadmissible, even where it is clearly relevant, or indeed decisive, from a logical or 'common sense' perspective.

The law of evidence under the common law system, which is characterized by the wealth, the precision and the technicality of its rules, contains two fundamental principles that appear to constitute major obstacles to the admissibility of computer and telematic

documents as evidence of the information they contain. These rules are the hearsay rule and the best evidence rule.[45]

(a) Hearsay rule. By virtue of the hearsay rule, a witness can only testify on the basis of his personal knowledge, permitting his statements to be verified by cross-examination. In principle, the court should not be invited to rely upon the truth of a factual assertion, unless that assertion comes from a witness who is testifying in court, on the basis of first-hand knowledge. Traditionally, the form of evidence preferred by judges was indeed oral testimony given by live witnesses, in order that the veracity of the witnesses and their credibility might be tested by rigorous and sometimes withering, cross-examination.

Oral evidence is therefore only admissible if it is given by the person with the personal knowledge of the facts being asserted. Knowledge from secondary sources, such as other persons, books or records is regarded as 'hearsay evidence' and is, in principle, inadmissible. Information that the witness heard someone else say—referred to as 'hearsay'—would be excluded, given that such other person should be compelled to testify firsthand so that, again, the reliability testing mechanism of cross-examination could be brought to bear.[46]

Applied to written evidence, this rule means that a document is not admissible unless its author is present to testify before the court on its content. The actual author of the document should also have to appear personally in court. Because by their nature computers cannot be cross-examined, legal writers and the case law have always considered computer documents to be hearsay evidence.

(b) Best evidence rule. In determining admissibility of evidence, English courts have long adopted the 'best evidence rule'. This rule means that the court will give most credence to the best evidence available, such as original documents or oral testimony. By virtue of the best evidence rule,[47] a document is in principle only admissible if it is produced in its original version. Computer documents are often only transcriptions of 'traditional' documents (bills, orders, forms, etc.), which constitute the originals; these are often destroyed after being recorded on a computer. Even when there is no written document that could serve as the basis of a computer document, the original is considered to be the data contained in the computer in magnetic or electronic form and the machine printout on which the data appears in readable form is only a transcription of that data, and as such, is not admissible before a court.

Exceptions. Fortunately, there are in English law numerous exceptions to the best evidence and hearsay rules. In the absence of such exceptions, there would be relatively little scope for the use of computer evidence in English trials. Unfortunately, however, the scope of the various exceptions depends on rules of evidence that are often no less technical than the exclusionary rules themselves.[48]

(a) Exceptions to hearsay rule. There are several exceptions to the hearsay evidence rule, such as the 'business records exception' (a business record created in the course of everyday commercial activity can be introduced as a piece of evidence, even if there is no individual who can testify on the basis of personal knowledge), or the 'photographic copies exception'.

In this context, the question whether computer files and printouts are inadmissible hearsay evidence or fall under one of these exceptions has been subject to extensive

debate.[49] In the common law system, the hearsay and best evidence rules theoretically prevent the admissibility of computer documents before the courts.

In the absence of jurisprudential exceptions to the hearsay rule granting the admissibility of computer documents as evidence of the facts that they contain and given the fact that it is impossible for the courts to create new exceptions to this rule, the legislator intervened in 1968 and introduced, along with new general provisions relating to hearsay evidence, provisions relating specifically to computer documents. Section 1 of the Civil Evidence Act (1968), which governs civil proceedings before the High Court, the county courts and some tribunals provides that a statement, other than one made by a person while giving oral evidence in the proceedings, may only be admitted as evidence of any fact stated therein to the extent that it is admissible under the Act or some other legislation. In its provisions of general application, the Civil Evidence Act (1968) allows the admissibility of 'first-hand' hearsay. Section 5(1) of the Act provides that:

> A statement contained in a document produced by a computer shall, subject to rules of court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it shows that the conditions mentioned in subsection (2) are satisfied ... .

Applied to computers, this rule means that a computer document is admissible if the person who loaded the data had a personal knowledge of it, or acting in the exercise of his duty, received it from a person who had such knowledge. The Civil Evidence Act lays down specific conditions relating exclusively to the admissibility of evidence in the form of computer documents (even if it does not provide any definition of the electronic evidence[50]). By virtue of these conditions, a computer document will be admissible as evidence if it was produced by a computer operating properly, which is regularly used for the normal activities of its user and supplied with information of the kind contained in the document put forward as evidence. Moreover, the information contained in the document must reproduce the information supplied to the computer. A certificate identifying the document, describing the manner in which it was produced and any device involved in its production as well as any other useful information relating to the conditions of the storage of the data, must be submitted to the court, signed by a person occupying a responsible position in relation to the operation of the relevant process or the management of the relevant activities. A computer printout or display showing information automatically recorded by the computer itself, or by machines or sensors linked to it, is no more hearsay than a film or audio tape recording an incident. In jurisdictions that have to date not implemented, or in the future do not implement evidence law provisions taking cognisance of computer-generated evidence in their evidence law statutes,[51] parties arguing for the admissibility of computer-generated records tend to rely on either the statutory business record rules in the various evidence acts or on the common law business records exception to the hearsay rule. Generally, courts have expressed very little reluctance to admit computer-generated records.[52]

(b) Exceptions to the best evidence rule. The production of a copy as evidence of the contents of its original is permitted if the party exercising this right establishes that he was unable to obtain the original. Thanks to its very general terms, this exception allows the removal of the obstacles created by the best evidence rule to the admissibility before the courts of computer documents. To establish their non-availability, it is enough to show that the originals of such documents were destroyed in the normal course of business or never existed. Furthermore, section 5 of the Civil Evidence Act (1968) provides that copies of electronic documents are admissible if their conformity with these documents are sufficiently established.

Relevance—A relevant fact, sometimes called a 'fact relevant to the issue', an 'evidentiary fact' or '*factum probans*', is a fact from which the existence or non-existence of a fact in issue may be inferred. If the only facts that were open to proof or disproof were facts at issue, many claims and defences would fail. Very often, the only available evidence is that which can establish some other facts or facts relevant to the fact at issue. Evidence of relevant facts is described as 'circumstantial evidence'.

If a computer document satisfies the conditions of admissibility as described above, it is declared admissible and it is then for the court to weigh up its probative value taking into account all the circumstances, notably the degree of simultaneity between the occurrence of a fact and its recording on computer as well as any interest that any person who is implicated might have in altering the data.

The judge decides freely about the relevance of the evidence brought to him by the parties. Since there is no strict legal rules of the evidence and as the judicial system is mainly based on accusatorial mechanisms, English judges may freely appreciate the relevance of the proofs. Evidence must be sufficiently relevant to be admissible and sufficiently relevant evidence is only admissible in so far as it is not excluded by any rule of the law of evidence. The consequence, of course, is that some relevant evidence is excluded.

2.2.5. Electronic evidence in criminal cases

2.2.5.1. *Continental law countries (Belgium, France, Italy). Burden of proof*—In criminal cases, the legal burden of proving any fact essential to the prosecution case rests with the prosecution and remains with the prosecution throughout the trial. This is a logical consequence of the presumption of innocence. Authorities in charge of the prosecution must prove the existence of offences they are prosecuting while the accused bears no legal burden in respect of the essential ingredients of an offence, whether they be positive or negative and whether or not he denies any or all of them. Even if it might happen in some cases that a civil party contributes to establishing the reality of an offence, there is in criminal cases no legal distribution of the burden of proof between opposing parties.

The authorities in charge of the prosecution thus have to prove all the ingredients of an offence and to disprove any justification cause put forward by the prosecuted.

As result of this, in case of any doubt, the judge has to acquit the defendant.

Admissibility—Continental law countries (and many others) operate according to the principle of free introduction and free evaluation of evidence ('*système de l'intime conviction*'[53]). Because there are no strict legal rules concerning the admissibility of evidence in these law systems,[54] the judge (or the jury, in high criminal cases before Crown court or *Cour d'assises*) is in principle allowed to use all kinds of evidence. Even so, one can ask how electronic evidence is going to be considered by the court.[55] Contrary to the civil system, where legal evidence is compulsory, criminal law establishes the liberty of proofs. It means that in criminal cases, every means of proof is in principle permitted as far as it is gathered according to specific rules and respecting general principles of law. In this system of intimate conviction, the judge estimates in his conscience whether the offence exists or not. He has the full liberty to appreciate the relevance of the gathered evidence.

In these legal systems, the electronic evidence derived from computer records is in principle admissible.

In Belgium—In the Belgian law system, there is no legal system regulating the admissibility of the evidence before a court. Belgian rules relating to the evidence in criminal cases are not legalist.[56] The *Code d'instruction criminelle* just holds a very few dispositions relating to the admissibility of evidence[57] so that the gathering and the production of evidence is usually described as '*free*' in Belgian criminal law. In principle, every piece of evidence is supposed to be admissible and valid as far as it results from rational thoughtfulness and was collected in a regular way.[58] Article 342 of the *Code d'instruction criminelle* concerning the procedure to be followed by the jury before the *Cour d'assises* lays down that the jury has to decide following its '*intimate conviction*'. This article is usually interpreted in a broad way, and is considered as the foundation of the legal rule permitting the free collection of the evidence in criminal cases, as well as before tribunals and courts with no jury. This has become a general principle in criminal law. In the case of regular gathering the evidence, the judge has to decide on the guiltiness of the defendant, who can only be condemned if the judge (or the jury) become *intimately convinced* of the defendant's guilt.[59]

The choice of the means of proof is therefore seen as '*free*', even if the judge remains unable to appreciate the probative value of each piece of evidence provided.

In France. The French legal system institutes the freedom of the proof in criminal cases. Article 427 of the French *Code de procédure pénale*[60] lays down that: '*Hors le cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction*'. This can be translated as follows: 'Except for particular legal dispositions, offences can be demonstrated by every means of proof and the judge decides according to his intimate conviction'. Every means of proof is thus in principle permitted as far as it is gathered, according to specific rules and in respect of the general principles of the law. In this system, based on the intimate conviction of the judge, the judge has to act according to his conscience and to estimate, on the basis of the pieces of evidence brought to him, whether an offence exists or not.

In Italy. The basic operation and outline of the Italian criminal justice is determined primarily by the Code of Criminal Procedure enacted in 1930.[61] This Code has been amended several times, one major amendment was passed in 1955. Police services are in charge of preliminary investigations of alleged offences and detection of their perpetrators, including the collection and holding of evidence. The police are obliged to report to the judicial authorities all offences involving *ex officio* prosecution which comes to their attention.

The Italian procedure code devotes a whole book to the issues of proof. Articles 187–193 hold general dispositions laying down general principles of the evidence, articles 194–243 hold the regulations of the means of proof and articles 244–271 hold rules relating to the means of seeking pieces of evidence. According to article 189 CPP, the judge may use every piece of evidence brought to him, even if one or more pieces of evidence were not foreseen by the law, as far he considers this evidence as relevant to establish facts or to verify them.

Judicial proceedings begin with a preliminary judicial investigation. In the case of flagrant offences—offences admitted by the suspect or demonstrated by clear evidence—the investigation is conducted by a magistrate of the public prosecutor's office ('*istruzione sommaria*'). In all other cases, the investigation is carried out by an investigating judge ('*istruzione formale*'). It is the public prosecutor who decides which of the two procedures is to be followed, but a suspect may request that the investigating judge undertakes the preliminary enquiry. If the suspect is in custody, the investigation must be carried out by the investigating judge if, after 40 days, the public prosecutor has not asked for discharge or trial. As in France, the Italian criminal procedure code lays down the principle of the freedom of the proof in criminal cases: any piece of evidence is in principle admissible, as far as it is not illegal in itself and fulfils two conditions. First, it has to make the facts certain and second, it cannot result in damage to the moral liberty of the prosecuted person (article 189, 1, of the *Codice del rito penale*). As for the system of '*intime conviction du juge*' that dominates Belgian and French legal systems, the Italian judge assesses the relevance of the evidence that is brought to him. He must nevertheless motivate his decision concerning the relevance he gave to each means of proof (article 192, 1, of *Codice del rito penale*). Moreover, he may not decide about the existence of a fact by way of pieces of evidence, unless these are serious, accurate and corroborating (article 192, 2, of the *Codice del rito penale*).

However, this 'liberty' does not mean that the evidence is in any case valid. Views differ indeed on the desirability of admitting evidence that has been obtained illegally (for example by a crime, tort or breach of contract or in contravention of statutory or other provisions governing the powers and duties of the police in investigating crimes) or improperly (for example by trickery, deception, bribes, threats or inducements). At one extreme, the view is taken that evidence that is relevant and otherwise admissible should not be excluded because of the means by which it was obtained: to exclude, it would, in some cases, result in injustice including the acquittal of the guilty party. If this opinion is favoured, all evidence that is necessary to enable justice to be done should be admitted. At the other extreme, however, one can think that illegally or improperly obtained evidence should always be excluded; to admit it might encourage the obtaining of evidence by such means. Following this opinion, all such evidence should be excluded, even if it sometimes results in injustice.[62]

Laws of evidence represent in many countries a compromise between those two extreme views. Problems may occur when procedural provisions provide specific regulations for the proof of judicial acts, or proof of legal documents.

In Belgium. Even if the gathering and the production of pieces of evidence is usually seen as '*free*' in criminal cases, the Belgian Supreme Court (*Cour de cassation*) decided many years ago that irregular pieces of evidence had to be ruled out.[63] According to decisions of the Belgian Supreme Court, a piece of evidence becomes irregular when it was gathered in a way that is expressly unlawful, or in a way that is not in accordance with substantial rules of criminal laws or general principles of the law and, more specifically, with due respect to the rights of the defence.[64]

Non-observation of legal requirements relating to the admissibility of the evidence. The Belgian judge is forced to base his decision on pieces of evidence gathered in a licit and regular way by the pursuing party. Invalid pieces of evidence should be considered as those gained as a result of an infringement (such as violation of the professional secrecy, as a result of a theft, an illegal phone tapping, menaces, malicious wounding, etc. Invalid pieces of evidence can never lead to a verdict. Furthermore, if the means of proof becomes strictly regulated (such as a search or a corporal exploration) only lawfully gathered pieces of

evidence are seen as valid to justify a prosecution. For example, information gathered as a result of illegal interception of telecommunications (or e-mails) can never be used by the judge to motivate a prosecution.

With regard to electronic evidence, the Belgian Parliament adopted on 28 November 2000 a specific law relatint to computer crime called '*Loi relative à la criminalité informatique*' (cyber crime Act).[65] This law contains two types of rules. The first type (substantive criminal law) edicts new incriminations that may occur only in the cyber world (computer forgery, computer fraud, internal and external hacking and computer sabotage) and adapts existing rules to the peculiarities of this environment. The second type (procedural law) introduces new dispositions of procedural law and edicts the methods that may be used by the public authority for the prosecution and the enquiry of computer related criminal cases.

As far as procedural law is concerned, these dispositions give the pursuing party (the prosecution, ie *le Ministère public* or *le Procureur du Roi*) new and important prerogatives for the gathering of electronic evidence. More specifically, the law allows the prosecution to seize data stored on corporal data carriers (by way of copying them and blocking their access), to seek networks (in respect of the dispositions relating to the house search) even if the servers that store the data are located abroad, to require the participation of experts to solve technical problems and to allow, to a certain extent, wiretapping.[66]

Violation of the general principles of law. In the last few years, case law has increasingly put forward dispositions of the European Convention on Human Rights and the principle of the respect due to the rights of the defence to justify the dismissal of some pieces of evidence.[67] A piece of evidence obtained in a way that is not in accordance with general principles of the law relating to the judicial criminal procedure, has to be declared illegal, even if the way used to collect the proof is not unlawful in itself. If the methods of investigation or the conditions of collecting pieces of evidence were unauthorized, this evidence is vitiated so that it cannot be accepted as proof and any judicial decision based on it should be declared invalid.

In France. The liberty of proof in criminal cases has some limitations. First, the gathering of pieces of evidences cannot attempt to undermine fundamental human values. Second, pieces of evidence must be obtained in a lawful way. Third, no violation of the general principles of law can occur in that process.

Respect of fundamental values. The prosecution of offences cannot attempt to undermine fundamental human values. In that way, the moral and physical integrity of the person may not be affected. For instance, French jurisdictions condemn disloyal processes used to gather evidence.[68] French courts declared thereby that statements of the accused gained as a result of violence must be considered inadmissible as evidence.[69]

Lawful character of the gathering of evidence. Despite the principle of the liberty of proof in criminal cases, pieces of evidence presented to the judge must have been gathered in a lawful way. If not, they have to be ruled out of court. The process of obtaining pieces of evidence must thus not have itself led to any infractions. Moreover, the legal conditions foreseen for every particular means of proof must have been strictly observed.

The electronic environment brings specific difficulties for the gathering of pieces of evidence. To cope with the increase in new problems, the French legislator quite early on (5 January 1988) adopted the *Loi Godfrain relative à la fraude informatique*[70] (the

Computer Fraud Act), which defines specific offences to prevent any attempts to fraudulently access/alter automated data systems that are now part of the criminal code (see eg articles 323-1, 323-2 and 323-3 of the French criminal code introducing respectively, fraudulent access into automated data systems, intentional infringement to such a system and intentional infringement to data stored on it).[71] It also created two new services with particular competences and technical means in order to fight against cybercrime.[72] Meanwhile, no particular procedural tools for the gathering of on-line evidence have been created.

However, evolution of information technologies have made the creation of specific procedural instruments unavoidable. Therefore, the French Parliament elaborated a '*projet de loi de la Société de l'information*' (Information Society bill), aiming to provide police services and prosecution authorities with procedural instruments to cope with cybercrimes. Unfortunately, the bill was declared null and void, and it took a further 10 years for the three main themes of the bill to be reutilized in the *Loi sur la sécurité quotidienne* (the Daily Security Act) adopted on 15 November 2001.[73]

Beside new instruments, such as the possibility of hearing a witness or a prosecuted party by way of videoconferencing (article 32 of the *Loi sur la sécurité quotidienne*), law enforcement agencies now have the ability (as result of three amendments to the article) to consult previous Internet traffic data.[74] Despite the general principle of the erasing traffic data by Internet service providers, telecommunication operators may indeed be forced, in specific cases and as result of court orders, to save traffic data information for a period of at least one year. Furthermore, police services are now allowed to decode data collected during judicial or security interceptions or during search or seizures (article 30 and 31 of the *Loi sur la sécurité quotidienne*, introducing new articles 230-1 to 230-5 to the code of criminal procedure, new article 11-1 to the *Loi n°91-646 du 10 juillet 1991, relative au secret des correspondances émises par la voie des télécommunications* and a new article 434-151 to the French criminal code).[75] We should however point out that the French law does not provide any dispositions relating to online search or seizure of data.[76] This means that seizures in the field of cyber crime remain attached to the rules of seizure in the corporal environment and that law enforcement agencies are only empowered to seize corporal objects (supports for data), such as computers, servers, etc.

As far as judicial and security interceptions are concerned, these were already foreseen by the *Loi 91-646 du 10 juillet 1991, relative au secret des correspondances émises par la voie des télécommunications* (Secret of Telecommunication Correspondences Act). Judicial interceptions can be decided in case of infringements that are liable to at least two years of imprisonment (article 100, French criminal code). Security interceptions which intend to collect information that could be of interest for the National Security (articles 3–19 of the *Loi 91-646 du 10 juillet 1991*) need a written and motivated authorization of the Prime Minister, taken on a written and motivated proposition of both Ministers of Defence and Home Affairs.[77]

Violation of the general principles of the law. As in Belgium, evidence gathered in a way that is not in accordance with the general principles of the law relating to the judicial criminal procedure, must be declared inadmissible, even if the way used to reach the proof is not unlawful in itself. For example, pieces of evidence that were not submitted for cross-examination of the parties or that were not correctly communicated cannot be used as a basis for a prosecution.

In Italy. The Italian law system institutes (article 189, 1, of the *Codice del rito penale*) the liberty of proof in criminal cases, meaning that any evidence that was not expressly declared unlawful by the law can be used in criminal cases. However, this liberty remains bounded by some limitations, according to the type of proof concerned. The Italian law system distinguishes two kinds of proof: those that are specifically provided by the law, and those that are not.

For the legally foreseen pieces of evidence (provided by the Italian law), the judge must verify that they conform with legal requirements. In that way, for instance, the interception and tapping of telecommunications may not be used for any type of infringement for it must conform with conditions stated by the *Legge 23 dicembre 1993, n. 547, recente modificazioni ed integrazioni alle norme del codice penale e di procedura in tema di criminalità informatica.*[78] This law concerns the interception of telecommunications and wiretapping (article 266 C.P.P.). Furthermore, pieces of evidence gathered in breach of other legal interdictions cannot be used (article 191 of the *Codice del rito penale*).

The law can expressly exclude some pieces of evidence. When a piece of evidence is considered as superfluous or obviously irrelevant, the judge is not allowed to use it and this piece of evidence has to be ruled out of the case (article 190 of the *Codice del rito penale*). As the Italian law system does not accept the principle: '*male captum, bene retentum*', the judge has to order the dismissal of inadmissible pieces of evidence. Article 191 of the criminal code lays down that proof gathered in a way that is not in accordance with legal interdictions cannot be referred to, either for the trial, or for any decision concerning indictment. The judge may not use any results gained *contra legem*. All parties at the trial may ask at any time for the dismissal of pieces of evidence gathered in an unlawful way. This means that it is not necessary to disqualify inadmissible evidence at the very beginning of the trial: there is no tacit agreement.

Relevance—In these systems based on the intimate conviction, the judge assesses according to his conscience whether the offence exists or not. He has the full liberty to appreciate the relevance of the gathered evidence.[79] He assesses the relevance of elements on which he used to base his decision, provided that these elements had been first submitted for cross-examination by the parties.[80]

2.2.5.2. *Common law country (UK—England). Burden of proof*—The contemporary English criminal process is accusatorial rather than inquisitorial. The case against an accused is investigated, prepared and directed through the courts by a party, usually a public official representing the Crown, and not by the judges or magistrates as in an inquisitorial system. In English law, the presumption of innocence is considered as a fundamental element. In principle, the burden of proof rests entirely with the prosecution. However, this principle has some exceptions. The burden of proof rests with the defendant if a special legal text expressely foresees it, when a text creates a general exception concerning the Summary trial, and in cases of mental disorder.

Admissibility—In England, there is no criminal procedure code.[81] Procedural rules are therefore deduced from decisions delivered by the Courts of Appeal and the House of Lords, as well as of statutes, particularly the Police and Criminal Evidence Act (PACE, 1984). However, although the English Parliament has adopted for the last 20 years several texts in the field of criminal and civil procedures with the intention of improving legislation

in some spheres that have been dealt with inadequately by current case law,[82] the English legal system remains mainly based on case law and more specifically on the law of the precedent: the courts remain bound by decisions taken by upper level courts. If the law has not solved a question yet, it is in the previous case law where the judge must find the solution of the conflict. The law system is then characterized by an oral and adversarial procedure. Rules relating to the evidence are thus scattered in a range of legal texts coming from the late XVII century[83] as well as in a huge jurisprudence. This makes the law of evidence difficult to describe.

Moreover, the European Convention for the protection of Human Rights and Fundamental Freedoms[84] does not have any direct effect on the English internal law system. The result is that it is impossible to use EU law as a source of the law of the evidence in English law: the courts always interpret English law in a way that conforms with the convention, but in case of conflict, English rules will always prevail.

The main guidelines of English rules relating to the admissibility of evidence in criminal cases may nevertheless be presented as follows. In principle, all relevant evidence is admissible in English law subject to exceptions. Evidence must be sufficiently relevant to be admissible, but sufficiently relevant evidence is only admissible in so far as it is not excluded by any rule of the law of evidence.[85] For the decisions relating to remanded custody and to punishment, all means of proof are admissible and may be used as far as applicable. This also includes pieces of evidence gained in violation of the law. In this second part of the trial (the determination of the punishment), all evidence is indeed admissible.

To establish guilt of an accused, some means of proof are not admissible, among which is hearsay evidence (see above) as well as that founded on previous convictions or on the personality of the accused. Under the adversary system of trial, the court itself cannot undertake a search for relevant evidence but must reach its decision solely on the basis of such evidence as is presented by the parties. The reason to exclude the hearsay evidence is clear: the person with the information is expected to testify and is not there at the hearing. It is then impossible for him to declare under oath and submit to cross-examination, which is one of the main principles of the English procedural system.

In Belgian, French and Italian law systems (see above), in order to condemn someone it is required that their culpability is demonstrated by the way of proof (pieces of evidence), mainly brought by the prosecution. In these French inspired systems, this legal obligation does not disappear when culpability is acknowledged by the accused. If culpability is acknowledged, their declaration will only be considered as just one more piece of evidence. Even in this case, the judge still remains free to decide on their innocence or culpability.[86] The English law system is, on this point, rather different. In England, like in other common law countries, the fact that the accused 'pleads guilty' is considered as decisive: the prosecution is released from supplying evidence and the court has to condemn the accused even if it is not ultimately convinced about their culpability. In the case of a 'guilty plea', the liberty of the proof regulates the admissibility of the evidence and, in theory, all evidence is admissible. This procedural particularity must not be undermined. In England, the legal rules related to the admissibility of judicial evidence are much stronger than in European continental law systems. As a vast majority of cases pass through the courts by way of a 'guilty plea', this exacting evidence law is fortunately not called upon in these cases.[87]

However, when the strict rules of evidence apply, they forbid the use of a set of categories of inadmissible evidence. Among these, the testimony of an incapable witness is

considered as inadmissible and hearsay evidence is also strictly forbidden. The notion of 'hearsay' covers a rather large area and it includes oral assertions from third parties, as well as written assertions of non-witnesses. Informal written documents as well as statements made by the police are then considered as hearsay evidences. Former statements of witnesses appearing before the court, except those in contradiction with their oral testimony before the judge, are in the same way suppressed. There are nevertheless large exceptions to the principle of the exclusion of the hearsay evidence.[88] The most important is probably the one created by the Criminal Evidence Act (1965), making records relating to trade or business admissible as evidence.[89] In case of violated rules of the evidence, this does not prevent the accusation from producing the litigious proof; but the court retains the discretionary ability to accept it or to refuse it. Unlike the French rules of evidence (according to which non-admissible evidence must be declared null and void, thus nullifying the subsequent procedure—see above), English rules never render void inadmissible evidence even though similar mechanisms exist.[90]

In this way, when the law exceptionally refers to the statement of a witness concerning the quality of evidence, courts in some cases may decide to deny it for non-observance of legal requirements. Furthermore, article 76 of the Police and Criminal Evidence Act holds that confession of the accused is not admissible as far as the prosecution is unable to demonstrate that this was not obtained by way of oppression, or as a consequence of a behaviour making the confession of the accused less credible. Article 78 of the Police and Criminal Evidence Act entitles the court to exclude any unfair evidence put forward by the prosecution: 'In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse affect on the fairness of the proceedings that the court ought not to admit it'.[91]

Article 78 mainly applies to confessions obtained by the police in violation of the rules of the Police and Criminal Evidence Act and the codes for the conduct of cross-examinations. Case law, still developing, indicates that the court must exclude confessions obtained in a way that fails to respect the substantial rules, in particular a failure to respect the rules on the writing of declarations by the police that undermines its reliability, and a failure to respect the right to the advice of a lawyer having allowed the police to persuade a silent suspect to speak.[92]

Cases on these matters appear to result in a pattern according to which evidence may readily be excluded where the police act in bad faith and in so doing prejudice the rights of the suspect or his ability to have a fair trial.[93] Where the police act in good faith, but wrongly, the court will determine whether proceedings are thereby rendered unfair. The power to exclude evidence is not intended to punish the police for a failure to observe the rules. In particular, a failure to record an interview and to show the record to the suspect is regarded as a grave breach because it prevents the court from verifying what actually occurred.[94] The decision of a trial judge whether to exclude evidence on the ground of unfairness is discretionary and appellate courts will not readily interfere with his exercise of discretion.[95]

In case of facts discovered on the basis of inadmissible evidence with regard to article 76, the situation is expressly provided for in the PACE. The fourth paragraph holds that: 'the fact that a confession is wholly or partly excluded in pursuance of this section shall not affect the admissibility in evidence of any facts discovered as a result of the confession; or where the confession is relevant as showing that the accused speaks, writes or expresses

himself in a particular way, of so much of the confession as is necessary to show that he does so'. However, 'evidence that a fact to which this subsection applies was discovered as a result of a statement made by an accused person shall not be admissible unless evidence of how it was discovered is given by him or on his behalf'.

As for clues discovered by other irregular means, such as a non-authorized search, for example, the courts refer some to article 78. The jurisprudence affirms that this article can be used to suppress any indication discovered by the police as a result of an illegal act or a behaviour exceeding its powers.[96]

In spite of these affirmations, however, English courts seem very little disposed to suppress any evidence for such motives. That English jurisprudence is willing to admit such evidence represents an important change of attitude, because for a long time English courts appeared to show no interest in the way that evidence had been gathered.[97]

If law enforcement agencies act in violation of the PACE, it is theoretically possible to pronounce a disciplinary sanction. Unlike the French system, English criminal courts are not empowered to impose disciplinary sanctions on police agents. These sanctions may only be imposed by the chief of the regional police or by a special court. Irregular search, seizure or arrest could nevertheless lead, theoretically at least, to a civil trial. For very obvious reasons, however, the victim who is condemned because of these irregular actions, so discovered, is generally badly placed to institute proceedings.

The cross-examination of the accused is settled in detail by the Police and Criminal Evidence Act (PACE) while the recording of telephonic communications is organized in a very strict manner in the Interception of Communications Act (1985). Until 1990 and the Computer Misuse Act (1990), specific computer related crime did not exist in the UK except under the provisions of the Data Protection Act (1984) and therefore the prosecution of infringements involving computers had to be based on the offences available under the existing body of law. The Act has simplified the position and criminalized the following actions:

- unauthorized access to computer material (s.1);
- unauthorized access with the intent to commit or facilitate the commission of further offences (s.2);
- unauthorized modification of computer material (s.3).

To prove that an offence has been committed, the following points must be demonstrated:

- the computer performed a function as a consequence of either access being attempted or actual access (s. 1 and 2);
- the access was unauthorized (s. 1 and 2);
- the person attempting access knew that it was unauthorized (s. 1 and 2);
- the access was a preliminary to committing or facilitating a serious offence (s. 2);
- the modification to computer material was or would have been caused (s. 3);
- the modification was unauthorized (s. 3);
- the person attempting the modification knew it was unauthorized (s. 3) and
- the intention of the modification was to impair the computer's operation (s. 3).

It is no easy matter to establish these points and, despite this law, the extent to which documents generated from information stored by electronic means might be admissible as evidence remains subjected to various interpretations in the English courts.

Relevance—Common law always agrees with the principle of the free appreciation of the evidence: it never used the theory of the legal proof. The court acknowledges freely the relevance of the evidence (see above).

There are nevertheless some exceptions to this rule, such as article 13 of the Perjury Act 1911, which claims that a witness's testimony is not sufficient for a condemnation for perjury. Since the rule forbidding prosecution on the basis of a child's deposition without taking oath (that was not corroborated) was abolished in 1988, it is no longer important in a case where corroboration is obligatory.

In principle, a criminal court must condemn the defendant only when the evidence concerning the offence has been proven *beyond reasonable doubt*.

For the defendant before the magistrates' court, the possibility exists, theoretically at least, to ensure that this level of proof has really been reached. In the case of prosecution at the magistrates' court, the defendant can request the reasons behind the verdict according to a so-called 'case state' procedure. If the defendant suggests that the proof of his infringement was not sufficiently established, the court is obliged to specify the proof on which it founded its verdict. The defendant who is convicted by a jury before the Crown Court, however, does not have this opportunity. At the end of the hearing, the judge is obliged to give to the jury an oral summary of the proof gathered in order to convince its members about the guilt of the accused. He also has to forbid the jury to pay any attention to any fact that was not considered as admissible evidence, and to warn it against the proof that was not accepted because of lack of corroboration. If these recommendations are incorrect, the accused may lodge an appeal against the verdict. However, if the recommendations were presented correctly, there is no verification whether the jury understood them, or even if it did understand them, nothing prevents the jury from underestimating them. A jury cannot be interrogated on the motives of its guilt verdict. On the contrary, anyone that attempts to discover the motives from them risks being pursued for infringement to the article 8 of the Contempt of Court Act 1981.

2.2.6. *Electronic evidence in ADR/ODR.* Parties in cyberspace are still seeking a fragile balance of power. Amidst a growing number of conflicts, certain actors—mostly proponents of network self-regulation—wishing to achieve an effective solution while avoiding traditional complex legal proceedings, advocate alternative dispute resolution services.[98]

Alternative Dispute Resolution (ADR) may be defined as new cost-effective and time saving way of settling disputes out of court (the ADR is thus a negotiation process willing to lead to an agreement between opposite parties[99]) while ODR (sometimes called e-ADR) is generally the electronic form of ADR. The ADR is an 'alternative' to the judicial dispute resolution, and therefore usually to State procedures. A very broad range of dispute-related services is offered. A quick survey of pertinent literature reveals that the term ADR (or ODR when offered online) is used for mechanisms as different as dispute prevention, ombudsman programmes, conflict management, assisted negotiation, early neutral evaluation and assessment, mediation/conciliation, mediation-arbitration, arbitration, expert-determination, etc. A first distinction is then drawn between, on the one hand, actual dispute resolution, which covers procedures intending directly to resolve conflicts and, on the other hand, services that could rather be considered as satellite functions, seeking to prevent disputes or to facilitate or improve their resolution, without actually resolving them.[100] These last mechanisms are out of the scope of the CTOSE project, so that legal issues relating to the evidence before these 'services' will not be examined here.

Among dispute-related services willing to solve conflicts, a main distinction has to be made between two major types: mediation and arbitration.

Mediation is a form of assisted negotiation where a third neutral party, the mediator, helps the disputants come to an agreement to resolve their conflict. While the mediator, having no decision-making power, never imposes a solution, the degree of his intervention can vary significantly, ranging globally from 'pure' mediation, where the mediator intervenes as little as possible, to 'muscle' mediation, where the neutral tries to force an agreement on the parties.[101] As mediation seeks much more to satisfy each party's interests rather than to adjudicate fair and legitimate rights, the procedure is governed by few rules: substantive state law applies only insofar as some types of agreements are prohibited, and no rule of evidence controls the process.[102] The mediator may thus in principle receive all kinds of evidence and appreciate freely their relevance.

While the gist of mediation is to take the parties to a common ground of mutually acceptable solutions, the conception of justice in arbitration is much more straightforward. It relies on the determination of who is right and who is wrong: arbitration adjudicates rights and therefore has different requisites for the quality of its justice. It is the ADR form that applies legal rules with the highest density and, therefore, is the mechanism providing the most formal justice. As it is the private equivalent of a court and its awards are binding like judgements, arbitration is submitted to comparatively strict rules for it to have its desired effects. Arbitration must be compliant with fundamental procedural rules, among which the opportunity for the parties to be heard. According to the English High Court, this includes the right for the parties to present their case (by granting them sufficient time to prepare their arguments), the existence of proper and proportionate means for the receipt of evidence and a summary nature of the proceedings (and in particular a limited availability of hearings).[103] In any event, the jurisdiction of an arbitral tribunal must be based on an agreement, a court order or a statute or treaty. According to arbitration based on an agreement, a court order or a statute, rules relating to the evidence will be determined by rules held in the agreement, the law or the convention of arbitration itself. It is therefore impossible to list an exhaustive collection of rules of evidence in the case of arbitration. Without prejudice of particular dispositions, as the arbitration takes formal justice as its model, rules of evidence will most generally square with legal ones and this is the reason for referring to chapter one concerning the admissibility of the electronic evidence before arbitral jurisdiction.

3. Conclusions

As demonstrated above, rules governing the admissibility of evidence are rather complicated and largely vary from one country to another. It is therefore difficult to present them fully. This paper has only aimed at introducing the core principles of admissibility of electronic evidence.

The conclusion that may nevertheless be drawn is that there is a definite need to ensure that for any collection of computerized data the rules governing the obtaining of the evidence are followed precisely. Consequences of illegally obtained proof can vary from case to case.

It is therefore highly recommended that people involved in the handling of electronic evidence are aware of and kept constantly updated on these specific procedures. This is particularly important with regard to jurisdiction in cross-border crime cases. Ideally, the duty of disclosure should be the same. The Commission is therefore preparing a proposal

for a Council framework decision on mutual recognition of pre-trial orders to obtain evidence (including that for cybercrime investigation) that will cover search and seizure orders and production orders.

Notes and References

1 This paper has been written in the context of the CTOSE project (IST programme), and it is an adaptation and briefing of deliverable 3.1 'Admissibility of electronic evidence'. It was the basis for the presentation at the CTOSE Conference. This paper, however, is solely the responsibility of the author and does not represent the opinion of the other contributors to the CTOSE project or of the European Community (EC). Its purpose is to present, as clearly as possible for people who are unfamiliar with legal matters, the main principles of the admissibility of evidence. To this end, some legal concepts have been simplified. I am particularly grateful to Antoine Misonne, Assistant in Criminal Law at the Faculty of law in Namur, for his substantial help and valuable comments during the drafting of this report. I also wish to express my gratitude to María Verónica Pérez Asinari and Jean-Marc Dinant for their enjoyable and highly professional collaboration on the CTOSE project.

2 M Robins 'Computers and the discovery of evidence—a new dimension to civil procedure' *Journal of Computer & Information Law*, Vol 17, p 412, 1999.

3 Because of new technical developments and the growing use of computers in all areas of economic and social life, courts and prosecution authorities depend to an increasing extent on evidence stored or processed by modern information technology. Aware of this development, the EC published in the *Official Journal* in 1995 a public tender on computer-related crime, finally awarded to the University of Würzburg in October 1996. This university presented on 1 January 1998, a report written under the direction of Professor U Sieber entitled: *'Legal aspects of computer-related crime in the information society—COMCRIME study'*. This report presents the legal aspects of the computer crime in several EU member States as well as in countries outside of the EU.

4 D Morrow 'The IT security professional as investigator', online: http://www.gocsi.com/sec.pro.htm (1 May 2000).

5 Sieber, *op cit*, note 3, p 101.

6 P Sommer 'Evidence in Internet paedophilia cases', p 2.

7 Sieber, *op cit*, note 3, p 32.

8 Sommer, *op cit*, note 6, p 2.

9 D Brezinski and T Killalea 'Guidelines for evidence collection and archiving', p 4, on-line: ftp://ftp.ietf.org/rfc/rfc3227.txt.

10 Law of evidence is probably one of the most complex legal issues.

11 Sieber, *op cit*, note 3, p 101.

12 For a deeper study of the legal matters relied to the handling of electronic evidence and the protection of the privacy, see María Verónica Pérez-Asinari 'Legal constraints for the protection of privacy and personal data in electronic evidence handling' *International Review of Law Computers and Technology*, Vol 18, No 2, 2004, pp 231–250.

13 Because of our oversimplification, many concepts may appear simpler than they really are. It is thus recommended, for further examination of legal issues, to refer to legal theoretical studies.

14 G S Takach, *Computer Law*, p 366, Irwin Law, Toronto, 1998.

15 A Kean *The Modern Law of Evidence* 5th edn, p 1, Butterworths, London, 2000.

16 Although division of common law systems into private and public law is referred to infrequently (a division is more often noted in terms of the law of tort or the law of property, all part of what is known as substantive, as opposed to procedural law) this report has been built on this main classification. In terms of evidence, there have always been significant differences between the rules of evidence in civil cases and those that govern criminal cases. In 1968, the Civil Evidence Act introduced major reforms that made it possible for hearsay to be admitted in civil courts in many circumstances where it would remain inadmissible at common law. These reforms were not, on the whole, matched by comparable changes to the hearsay rule in criminal cases. Were the system to be classified as public and private law, private law would include the law of contracts, tort and property. Additionally so categorized would be family law, succession and trusts. Criminal law would constitute a major part of the public law, which would further embody constitutional and administrative law, and procedure.

17 This principle has been confirmed as well in national constitutions (e.g. Italy) as in international treaties (ECHR).

18 There are some exceptions to this principle. In some legal systems, the judge and the defendant do not always remain passive. The Belgian and French criminal codes procedure so institutes the *'juge d'instruction'*. This is a judge empowered to interview witnesses and defendants after police enquiries and before the hearing, or to order a search or request for an expertise. Article 190 of the Italian procedure code uses the term of 'right of the proof' for the accused and article 38 of the law of application of this code provides the notion of 'defensive inquiry' permitting the lawyer to seek evidence or witnesses.

19 G Stefani, G Levasseur and B Bouloc *Procédure pénale* 13th edn, pp 34–35, Dalloz, Paris.

20 M Antoine, J-F Brakeland and M Eloy 'Droit de la preuve face aux nouvelles technologies de l'information' *Cahiers du CRID*, No 7, p 55, 1991.

21 Kean, *op cit*, note 15, p 20.

22 Continental law systems distinguish two different relevant concepts: *la valeur probante* and *la force probante*.

23 J F Stephen *Digest of the Law of Evidence*, 12th edn, art. 1.

24 M Storme, *De bewijslast in het belgisch privaatrecht*, Gand, Faculté de droit de l'Université de Grand, 1962.

25 Art. 1315 Code civil: *'celui qui réclame l'exécution d'une obligation doit la prouver; celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation'*.

26 M Clavie, 'La charge de la preuve: questions choisies en matière contractuelle', *La preuve*, Vol 54, p 12, March 2002.

27 Art. 1316-4 of the French civil code, introduced by the Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. n° 62 of 14 March 2000, p 3968).

28 Commercial law is separately administered in civil law nations.

29 G Raymond, *Droit civil* 3rd edn, Litec, Paris, p 59, 1996.

30 *Ibid*.

31 *Ibid*, pp 59–60.

32 Art. 5 of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures lays down that: '1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings. 2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification service-provider, or not created by a secure signature-creation device' (*Official Journal* L 013, 19/01/2000 pp 12–20).

33 See notably the project of the European directive, Common position (CE) n° 28/1999 taken by the Council on the 28 June 1999, *O.J.E.C.*, C 243/33, 27 June 1999 and the type-law on electronic commerce, adopted by the CNUCID in 1996.

34 J.O. n° 62 of 14 March 2000, p 3968.

35 Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, Moniteur Belge, 29.09.2001.

36 Decreto legislativo 23 gennaio 2002, n. 10 ; Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (G.U. n. 39 del 15 febbraio 2002). In order to conform its legislation to European standards, the Italian legislator adopted on the 23 January 2002 a *Decreto legislativo* (decree) transposing the European Directive 1999/93/CE on electronic signature. An electronic document is now considered as a mechanical reproduction in the sense of article 2702 of the *Codice civile* and has the same relevance as of the handwritten document. Moreover, the electronic signature linked to an electronic document gives it the same effect it would have in the paper world, as far as the signature obey to the conditions of advanced signature and has been guaranteed by an assented certificate provider.

37 E Caprioli 'Le juge et la preuve électronique', on-line: www.Juriscom.net, 10 January 2000, p 7; V Sédallian 'Preuve et signature électronique', on-line: www.Juriscom.net, 9 May 2000, p 2.

38 Caprioli, *op cit*, note 37, pp 8–10; Sédallian, *op cit*, note 37, p 2.

39 Directive européenne 1999/93/CE du Parlement et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, *J.O.*, n°L013, 19.01.2000, pp. 12–20.

40 Caprioli, *op cit*, note 37, pp 14–20; Sédallian, *op cit*, note 37, pp 3–6.

41 *Ibid*, pp 60–61.

42 *Ibid*, pp 61–62.

43 Caprioli, *op cit*, note 37, pp 10–13; Sédallian, *op cit*, note 37, pp 2–3.

44 M-A Glendon and M W Gordon *Comparative Legal Traditions in a Nutshell* 2nd edn, West Group, St Paul, MN, p 236, 1999.

45 B Amory and Y Poullet 'Computers in the law of evidence—a comparative approach in civil and common law systems' *International Computer Law Adviser*, No 4, p 7, 1987.

46 Takach, *op cit*, note 14, p 367.

47 The 'best evidence rule' is also called the 'primary evidence rule'.

48 It would be wrong to assume that computer evidence can only ever be admitted by way of some such exceptions. Not all computer evidence is hearsay: some can be classified as original or even 'real' evidence and can then be admitted on largely the same basis as a photograph or a tape recording of an incident. It depends on the way in which the computer has been operating, and in some cases, on the availability of supporting oral testimony relating to the input of data.

49 U Sieber *The International Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy* Wiley, Chichester, 1986, p 111.

50 For most purposes, the question of whether a given device is a computer has been left to be decided on a case by case basis.

51 Several common law jurisdictions have expressly taken cognisance of computer-generated evidence in their evidence law statutes. See e.g. law statutes in Quebec and New Brunswick.

52 Takach, *op cit*, note 14, p 372.

53 The Belgian Supreme Court declared ten years ago that: 'le juge apprécie la culpabilité du prévenu selon son intime conviction; il le condamne lorsqu'il a la certitude humaine qu'il s'est rendu coupable du fait mis à sa charge' (Cass, 10 November 1992, Pas, 1992, I, p 1247). Unauthorized translation: 'The judge freely appreciates the guilt of the defendant according to his personal appreciation of the evidence; he can only convict when he is convinced that the accused effectively committed the offence for which he is prosecuted'.

54 Even if the continental law countries adopted procedural codes, unlike the common law countries.

55 The judge has to weigh the extent to which he can rely on the evidence (especially his own observations, the statements of suspects, witnesses and experts, as well as written documents).

56 P Henry 'De l'intime conviction' in *Les droits de la défense en matière pénale—Actes du colloque des 30, 31 mai et 1er juin 1985* Barreau de Liège, pp 201–236; A L Fettweis 'La charge de la preuve en matière pénale et la présomption d'innocence' in *Les droits de la défense en matière pénale—Actes du colloque des 30, 31 mai et 1er juin 1985* Barreau de Liège, pp 133–157; P E Trousse 'La preuve des infractions' *Rev. dr. pén*, pp 731–766, 1959; R Screvens 'La preuve pénale en droit belge' in *La présentation de la preuve et la sauvegarde des libertés individuelles* Bruylant, Bruxelles, 1977, pp 55–90. See, *contra*, R Legros 'La preuve légale en droit pénal' *J.T.*, 1978, pp 589–595; J Messine 'La vie privée et le droit de la preuve en matière pénale' *Ann. Dr. Louv.*, 1984, pp 403–425.

57 Art. 154: 'les contraventions seront prouvées soit par procès-verbaux ou rapports, soit par témoins à défaut de rapports et procès-verbaux, ou à leur appui'.

58 H-D Bosly 'La régularité de la preuve en matière pénale' *J.T.*, pp 121–128, 1992; A de Nauw 'Les règles d'exclusion relatives à la preuve en procédure pénale belge' *Rev. dr. pén. crim.*, 1990, pp 705–724.

59 The rule of the intimate conviction is hold in article 342 of the criminal procedure code.

60 The French criminal procedure code is available on-line: http://www.adminet.com/code/index-CPROCPEL.html.

61 The Italian criminal procedure code is available on-line: http://www.camerapenale-bologna.org/codice_procedura_penale/codice_di_procedura_penale_index.htm#cpbo.

62 Kean, *op cit*, note 15, p 49.

63 Cass., 27 February 1985, *Rev. dr. pén. crim.*, 1985, p 694.

64 Cass., 13 May 1986, *Rev. dr. pén. crim.*, 1986, p 905; Cass., 4 January 1994, *Rev. dr. pén. crim.*, 1994, p 80: 'Est illégale la preuve obtenue non seulement par un acte qui est expressément interdit par la loi, mais aussi par un acte inconciliable avec les règles substantielles de la procédure pénale ou avec les principes généraux du droit et, plus particulièrement, avec le respect des droits de la défense'.

65 Loi du 28 novembre 2000 relative à la criminalité informatique, *Mon. b.*, 3 February 2001.

66 For a detailed approach of the law, see: T Laureys *Informatica criminaliteit* Mys & Breesch, Gand, 2001; C Meunier 'La loi du 28 novembre 2000 relative à la criminalité informatique' C.U.P., Liège, 2001; S. Dussolier and F de Villenfagne 'La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique', online: http://www.droit-technologie.org/dossiers/analyse_loi_281100_criminalite_informatique.pdf.

67 María Verónica Perez Asinari 'Legal constrains for the protection of privacy and personal data in electronic evidence handling' pp 35–37.

68 Crim., 12 June 1952, *J.C.P.*, 1952, II, p 7241.

69 Crim., 28 October 1991, *Bulletin d'information de la Cour de cassation*, 15 January 1992, p 11.

70 Loi 88–19 du 5 January 1988, relative à la fraude informatique, *J.O.*, 6 January 1988.

71 T Verbiest and E Wéry *Le droit de l'internet et de la société de l'information*, Larcier, Bruxelles, 2001, pp 38–41.

72 Forum des droits sur Internet *Dossier 'cybercrime et démocratie'* www.foruminternet.org, October/November 2001, p 4; Verbiest and Wéry, *op cit*, note 72, pp 41–42.

73 Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, www.assemblée-nationale.fr.

74 Forum des droits sur Internet, *op cit*, note 73, pp 6–8; J-W Noël *Internet & enquête judiciaire*, pp 3–4.

75 Forum des droits sur Internet, *op cit*, note 73, pp 8–11; Noël, *op cit*, note 75, pp 4–6.

76 Forum des droits sur Internet, *op cit*, note 73, p 11.

77 *Ibid*, pp 8–10.

78 L M Marini *Internet e Intercettazioni, Internet e Legge Penale* G. Giappichelli, Turin, 2001, pp 173–192.

79 *Ibid*, pp 44–48.

80 Cass., 6 September 1971, *Pas.*, 1972, I, 12.

81 Scotland adopted the *Criminal procedure (Scotland) Act* 1975.

82 See *inter alia* the Police and Criminal Evidence Act (1984; sections 19, 20, 21 and 78), the Prosecution of Offences Act (1985), the Regulation of Investigatory Powers Act (2000), the

Computer Misuse Act (1990; sections 1, 2, 3, 10 and 17), the Copyright Designs and Patents Act (1988; sections 107, 108 and 109), the Telecommunications Act (1984; sections 42, 42A, 43, 44 and 45), the Post Office Act (1953; section 11), the Data Protection Act (1984), the Interception of Communications Act (1985), the Protection of Children Act (1978, section 1), the Anti-terrorism, Security and Crime Act (2001), etc. This list is by no means exhaustive.

83 The main historical sources of the English criminal procedure are: *History of the Pleas of the Crown* (Sir Matthew Hale, 1609–1676), *A Treatise of the Please of the Crown* (William Hawkins, 1673–1746), *Please of the Crown* (Sir Edward Hyde East), *The Petition of Rights* (7 June 1628), *The Habeas Corpus Act* (1679) and *The Bill of Rights* (13 February 1689).

84 The full text is available on-line: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

85 Kean, *op cit*, note 15, p 25.

86 M Delmas-Marty *Procédures pénales d'Europe* P.U.F., Paris, 1995, p 516.

87 More than 70% of the cases judged by the Crown Court and more than 80% of the cases judged by the magistrates' courts.

88 There are a number of overlapping common law rules and statutory provisions, some specifically concerned with one particular kind of document and others concerned with a wide range of documents. None of these are specifically concerned with computer-generated evidence. Because of the mainly jurisprudential character of these exceptions, it is rather difficult to list all of them in an exhaustive way. According to an English lawyer, there are 12 of them, while an American law writer distinguishes 45 exceptions. It is nevertheless true that in criminal cases, there is no legal statutory provision comparable to section 1 of the Civil Evidence Act, upon which the admissibility of computerized hearsay evidence can be said to depend.

89 However, the courts did not make a consistent distinction between documents that might or might not be hearsay. In *R* v *Pettigrew*, the court of appeal rejected a computer printout of banknotes on the ground that it did not come under the exception under hearsay. However, the court changed its position in a subsequent case.

90 Under the Police and Criminal Evidence Act (1984), a suspect has the right not to be held incommunicado, save in exceptional circumstances and to the advice of a lawyer. He also has the right to silence and rights intended to ensure his fair treatment. Breaches of these rights by the police may result in evidence being excluded at trial. In case of inadmissible evidence, English exclusionary rule does not render the evidence null and avoid but excludes it from the process.

91 The full text of the Police and Criminal Evidence Act is available on-line: http://www.swarb.co.uk/acts/1984PoliceandCriminalEvidenceAct.html.

92 *Reg* v *Samuel* (1988) 87 Cr App R 233; *Reg* v *Allardice* (1988) 87 Cr App R 380.

93 L Leigh 'Criminal law and procedure, common law jurisdictions' *Rev. int. dr. pén.*, p 424, 1992.

94 *Reg* v *Chung* (1991) 92 Cr App R 314; *Reg* v *Dunford* (1990) 91 Cr App R 1509; *Reg.* v *Canale* (1990) 91 Cr App R 1.

95 Leigh, *op cit*, note 94, p 424.

96 E.g. *DPP* v *McGladrigan* (1991) 155 JP 785.

97 *Crompton J, en Leathem* (1861) 8 Cox CC 498.

98 V Tilman 'Arbitrage et nouvelles technologies: Alternative Cyberdispute Resolution' *Ubiquité*, F.U.N.D.P., Namur, 1999, pp 47–64.

99 J El-Hakim 'Les modes alternatifs de règlement des conflits dans le droit des contrats' *R.I.D.C.*, 1997, p 347.

100 T Schultz 'Online dispute resolution: state of the art, issues, and perspectives—where are we ? And where are we going?' Report of the E-law colloquium, 16 November 2001, Geneva.

101 A Bevan *Alternative Dispute Resolution* Sweet & Maxwell, London, 1992, pp 15–16.

102 P R Fisher 'All you need to know about mediation but didn't know to ask—a parachute for parties in litigation!', available online: http://www.mediate.com/articles/fisher2.cfm.

103 *Walkinshaw* v *Diniz*, Unreported decision, High Court of Justice—Commercial Court (19 May 1999) 1999, Folio No 522; J Thomas *Arbitration International*, Vol 17, No 2, 2001, pp 193–210.